DOD PRIVACY IMPACT ASSESSMENT (PIA)

1. Department of Defense Component

U.S. Army, Assistant Chief of Staff for Installation Management (ACSIM), Family & Morale, Welfare and Recreation Command

2. Name of Information Technology (IT) System (APMS System Name)

Army Risk Insurance Management System (AREV)

3. Budget System Identification Number (SNAP-IT Initiative Number).

9990

4. System Identification Number(s) (IT Registry/Defense IT Portfolio Repository (DITPR))

582

5. IT Investment (OMB Circular A-11) Unique Identifier (if applicable).

N/A

6. Privacy Act System of Records Notice Identifier (if applicable)

A0608-10 CFSC, Child Development Services (CDS) (February 22, 1993, 58 FR 10002).
DOL/GOVT-1,Office of Workers' Compensation Programs, Federal Employees' Compensation Act File (April 8, 2002, 67 FR 16815).

7. OMB Information Collection Requirement Number (if applicable) and expiration date.

N/A

8. Type of authority to collect information (statutory or otherwise)

5 USC 8171-8173 (NAFI Act)
33 USC 901 et seq (Longshore Act)
20 CFR 701 et seq. (Longshore Act)
AR 215-1, Military Morale, Welfare, and Recreation Programs and Nonappropriated Fund Instrumentalities

9. Provide a brief summary or overview of the IT system (activity/purpose, present life-cycle phase, system owner, system boundaries, and interconnections, location of system and components, and system backup).

Advanced Revelation (AREV) is a DOS-based system that is used to maintain insurance data, produce reports, and pay insurance claims. It was purchased in 1991, is owned by FMWRC, and is located on a server in Alexandria, VA. Connection is made using the FMWRC Network. AREV is not connected to any other system or network, and is not accessible from any other network. System backup is done by both the Risk Management Office and Information Management Office. A summary of System Privacy functions follows: payment of insurance claims, maintain database for Family Child Care (FCC) providers/ issue FCC certificates, unemployment and Worker's Compensation verification. All users are Risk Management employees. Privacy system input/output are claim payments, reporting functions, and FCC certificates. The present life-cycle phase is operations and support.

10. Describe what information in identifiable form will be collected and the nature and source of the information (e.g., names, Social Security Numbers, gender, race, other component IT systems, IT systems from agencies outside DoD, etc.).

Names, Social Security Numbers, Gender, individual's address are collected and may be used to verify the identity of an individual and to make payments to the individual under the property liability program. From the report of injury, the date of injury, the claimant/employee, social security number, type of injury, claimant number, verification if report received and verification of service fee paid. This system may contain data from the report of injury filed on behalf of the employee seeking benefits under the Nonappropriated Fund Instrumentalities (NAFI) Act, which extends the provisions of the Longshore Harbor Worker's Compensation Act (LHWCA). A third party administrator (TPA) which is under contract with Department of Army adjudicates worker's compensation claims.

11. Describe how the information will be collected (e.g., via the Web, via paper-based collection, etc.).

The data is collected from Civilian Personnel Offices, Installation Judge Advocate General offices, and Installation Child Care Offices. Information is collected via paper-based, email, and fax. Data collection is to verify that the claimants are NAF employees and used to process the payment. All information is faxed, mailed or emailed to the Army Central Insurance Fund and comes from indirect sources.

12. Describe the requirement and why the information in identifiable form is to be collected (e.g., to discharge a statutory mandate, to execute a DA program, etc.)

Information is collected to identify individuals for claim payment or potential claim payments. The records maintained in this system are necessary to identify individuals

and make proper claim payment. AR 215-1, Military Morale, Welfare, and Recreation Programs and Nonappropriated Fund Instrumentalities, states the requirement for Family Child Care Providers to submit Social Security Numbers to the Risk Management Office. Social Security Numbers for Workers Compensation claimants are required by the Department of Labor Long Shore Act.

13. Describe how the information in identifiable form will be used (e.g., to verify existing data, etc.).

To identify individuals for claim payment or potential claim payments.

14. Describe whether the system derives or creates new data about individuals through aggregation.

No additional, new reports are created using aggregate data.

15. Describe with whom the information in identifiable form will be shared, both within the Component and outside the Component (e.g., other DoD Components, Federal agencies, etc.).

AREV is totally contained within the FMWRC network and not shared by any other group. No feedback from any source is given. Information will be available to authorized users with a need to know basis in order to perform official government duties. Internal FMWRC investigation or audit, may include JAG and/or internal review auditors.

16. Describe any opportunities individuals will have to object to the collection of information in identifiable form about themselves or to consent to the specific uses of the information in identifiable form. Where consent is to be obtained, describe the process regarding how the individual is to grant consent.

All information is given with verbal permission and knowledge of the employee at the time the information is obtained. It is the responsibility of each collecting official to provide the individual with a standard privacy statement.

17. Describe any information that is provided to an individual, and the format of such information (Privacy Act Statement, Privacy Advisory) as well as the means of delivery (e.g., written, electronic, etc.), regarding the determination to collect the information in identifiable form.

It is the responsibility of each collecting official to provide the individual with a standard privacy statement.

18. Describe the administrative/business, physical, and technical processes and controls adopted to secure, protect, and preserve the confidentiality of the information in identifiable form.

Users are restricted by network password elements. A person must have a valid network account with specific permissions in order to access the AREV server and must have client software installed. Access is granted following an approval process, is limited, and is controlled at the network level. Once granted access to the server, all users have the same access to all modules of the AREV application. Controls in place to prevent misuse derive from the FMWRC network's defensive layers such as the intrusion detection and log auditing server. Names, Social Security Numbers and addresses are sent to this office via US mail, email and fax.

This system has a current certification and accreditation. The system resides on secure military installations within secured facilities.

19. Identify whether the IT system or collection of information will require a System of Records notice as defined by the Privacy Act of 1974 and as implemented by DoD Directive 5400.11, "DoD Privacy Program," November 11, 2004. If so, and a System Notice has been published in the Federal Register, the Privacy Act System of Records Identifier must be listed in question 6 above. If not yet published, state when publication of the Notice will occur.

A systems notice currently exists. Either the current notice will be amended to be more descriptive of this business practice, or an entirely new system notice will be developed.

20. Describe/evaluate any potential privacy risks regarding the collection, use, and sharing of the information in identifiable form. Describe/evaluate any privacy risks in providing individuals an opportunity to object/consent or in notifying individuals. Describe/evaluate further any risks posed by the adopted security measures.

Due to the level of safeguarding, we believe the risk to individuals' privacy to be minimal. There are no risks in providing an individual the opportunity to object or consent, or in notifying individuals. Risk is mitigated by consolidation and linkage of files and systems, derivation of data, accelerated information processing and decision making, and use of new technologies.

21. State classification of information/system and whether the PIA should be published or not. If not, provide rationale. If a PIA is planned for publication, state whether it will be published in full or summary form.

The AREV program privacy data is for official use only. The PIA may be published in its entirety.